UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/501,902	02/10/2000	Philip L. Bohannon	11-20-1-2-2	4531

7590 01/30/2004

Docket Administrator (Rm 3C-512)
Lucent Technologies Inc
600 Mountain Avenue
PO Box 636
Murray Hill, NJ 07974-0636

EXAMINER	
ALI, AHMEDUR R	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/501,902	Applicant(s) BOHANNON ET AL.	
	Examiner Ahmedur Ali	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 February 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. The application has been examined. Claims 1-39 are pending in this Office Action.

Priority

2. Applicant's claim for domestic priority under 35 U.S.C. 119(e) is acknowledged to Provisional Application Serial No. 60/128,413, filed April 8, 1999 and U.S. Provisional Application Serial No. 60/147,880 filed August 9, 1999.

Information Disclosure Statement

3. An initialed and dated copy of Applicant's IDS form 1449, Paper No. 2 and 3, is attached to the instant Office Action.

Claim Rejections - 35 USC § 112

4. The term "... compressed... and ...decompressing..." in claim 4 and 5 is a relative term which renders the claim indefinite. The term "compressed and decompressing is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For purposes of examination, the limitation of the claims is being interpreted as meaning encrypting and decrypting an encryption key.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-14,16, 19-23, 34, 37 and 39 rejected under 35 U.S.C. 102(a) as being anticipated by Kara (U.S. Patent No. 5,802,175). With respect to claim 1, Kara teach a method for generating a cryptographic key (see abstract; col. 2, lines 42-57) using at least one parameter comprising the steps of:

retrieving at least one cryptographic share from a memory location identified as a function of said at least one parameter (see col. 2, lines 42-67); and

generating a cryptographic key based on said at least one cryptographic share (see col. 2, lines 42-67).

6. Claim 2 rejected as above in rejecting claim 1, wherein said at least one retrieved cryptographic share is encrypted, said method further comprising the step of:

decrypting said at least one cryptographic share (see col. 3, lines 1-25).

7. Claim 3 rejected as above in rejecting claim 2, wherein said step of decrypting comprises the step of:

decrypting using a value computed as a function of said at least one parameter (see col. 3, lines 44-57).

8. Claim 4 rejected as above in rejecting claim 1, wherein at least one retrieved cryptographic share is compressed, said method further comprising the step of:

decompressing said least one cryptographic share (see col. 5, lines 13-26).

9. Claim 5 rejected as above in rejecting claim 4, wherein said step of decompressing comprises the step of:

decompressing said at least one cryptographic share using an index of said memory location (see col. 5, lines 13-26; col. 6,lines 42-57).

10. Claim 6 rejected as above in rejecting claim 1, wherein said at least one parameter represents at least one measurement of a physical property (see col. 4, lines 62-67 to col. 5, lines 1-6).

11. Claim 7 rejected as above in rejecting claim 1, further comprising the step of:

generating at least one index as a function of said at least one parameter; and using said index to identify said memory location (see col. 4,lines 62-67).

12. Claim 8 rejected as above in rejecting claim 7, further comprising the step of:

retrieving a cryptographic share from a memory location in the vicinity of said memory location identified by said index (see col. 6, lines 42-64).

13. Claim 9 rejected as above in rejecting claim 7, wherein said step of generating at least one index comprises the step of generating the same index for a set of parameter values (see col. 6, lines 42-64).

14. Claim 10 rejected as above in rejecting claim 9, wherein said set of parameter values are within a predetermined range of values (see col. 6, lines 17-41).

15. With respect to claim 11, Kara teach a data structure comprising:

a plurality of storage locations (see col. 4,lines 64-66; col. 5, lines 13-26);

a first subset of said plurality of storage locations containing valid cryptographic shares (see col. 5, lines 13-42); and

a second subset of plurality of storage locations containing invalid cryptographic shares (see col. 5, lines 27-42).

16. Claim 12 rejected as above in rejecting claim 11, wherein said first subset of storage locations correspond to storage locations which are expected to be accessed during a legitimate computer resource access attempt (see col. 1, lines 17-22; col. 2, lines 58-67; col. 3, lines 44-57) .

17. Claim 13 rejected as above in rejecting claim 11, wherein said second subset of storage location correspond to storage locations which are expected to be accessed during an illegitimate computer resource access attempt (see col. 1, lines 17-22; col. 2, lines 58-67; col. 3, lines 44-57).

18. Claim 14 rejected as above in rejecting claim 11, wherein at least some of said cryptographic shares are encrypted (see col. 8, lines 9-15).

19. Claim 16 rejected as above in rejecting claim 11, wherein at least some of said cryptographic shares are compressed (see col. 2, lines 58-67; col. 7, lines 21-26; Fig. 3).

20. With respect to claim 19, Kara teach a method for maintaining a data structure which has valid cryptographic shares stored in a plurality of locations, said method comprising the step of:

periodically changing the number of locations that contain valid cryptographic shares (see col. 2, lines 23-27, 42-67).

21. Claim 20 rejected as above in rejecting claim19, wherein the step of changing the number of locations that contain valid cryptographic shares comprises the step of:

storing invalid cryptographic shares in at least some locations which previously contained valid cryptographic shares (see col. 2, lines 42-67 to col. 3, lines 1-25).

22. Claim 21 rejected as above in rejecting claim 20, further comprising the step of:

storing said invalid cryptographic shares in locations which are not expected to be accessed in connection with an authorized computer resource access attempt (see col. 2, lines 42-67 to col. 3, lines 1-25).

23. Claim 22 rejected as above in rejecting claim 19, wherein said step of changing the number of locations that contain valid cryptographic shares comprises the step of:

storing valid cryptographic shares in at least some locations which previously contained invalid cryptographic shares (see col. 2, lines 42-67 to col. 3, lines 1-25).

24. Claim 23 rejected as above in rejecting claim 2, further comprising the step of:

storing said valid cryptographic shares in locations which are expected to be accessed in connection with an authorized computer resource access attempt (see col. 2, lines 42-67; col. 3, lines 36-57).

25. With respect to claim 34, a method for generating a cryptographic key using a plurality of parameters having a sequence and representing physical measurements, said method comprising the steps of: for each of said plurality of parameters; retrieving an encrypted cryptographic share from a memory location as a function of the sequence of said parameter; decrypting said encrypted cryptographic share with a function of said

parameter; and generating a cryptographic key using said decrypted cryptographic shares (see abstract; col. 2, lines 42-67 to col. 3, lines 1-25; col. 6, lines 30-64).

26. With respect to claim 37, a data structure for use in generating a cryptographic key based on n parameters representing physical measurements, said data structure comprising: n storage locations each associated with a respective one of said n parameters, each particular storage location containing an encrypted cryptographic share which was encrypted using an expected values of a function of the parameter associated with said particular storage location (see col. 2, lines 42-67 to col. 3,lines 1-25).

27. Claim 39 rejected as above in rejecting claim 37, wherein said cryptographic key may be generated using less than *n* cryptographic shares (se col. 3, lines 1-25).

Claim Rejections - 35 USC § 103

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

29. Claims 15, 18, 24, 26-27, 29-33 and 35 rejected under 35 U.S.C. 103(a) as being unpatentable over Kara U.S. Patent No. 5,802,175 in view of Brown et al. U.S. Patent No. 5,557,686 ('Brown' hereinafter).

30. As to claim 15, Kara teach the limitations as indicated above in claim 14.

Kara does not explicitly disclose the use of a password.

Brown disclose the use of a password (see col. 2, lines 52-56; col. 3, lines 35-41)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Brown within the system of Kara to arrive at the invention as claimed because the implementation of encrypting cryptographic shares with a password would prevent unauthorized users to attempt to access the cryptographic keys within the memory location and further provide an increased level of security of the combined system.

31. As to claim 18, Kara teach the limitations as indicated above in claim 11.

Kara does not explicitly disclose a vector space secret sharing scheme.

Brown disclose a vector space secret sharing scheme (see col. 2, lines 12-51; col. 5, lines 25-29; col. 6, lines 61-67).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Brown within the system of Kara to arrive at the invention as claimed because the implementation of a vector space would prevent unauthorized users to attempt to access the cryptographic keys within the memory location and further provide an increased level of security of the combined system.

32. With respect to claim 24, Kara teach a method for generating a cryptographic key (see abstract; col. 2, lines42-57) comprising the steps of:

generating a cryptographic key using said cryptographic shares (see col. 2, lines 42-57).

Kara does not explicitly disclose measuring a plurality of keystroke features during entry of a password and retrieving from a data structure a plurality of cryptographic shares as a function of said plurality of keystroke features.

Brown disclose measuring a plurality of keystroke features during entry of a password (see col. 2, lines 12-56; col. 3, lines 35-41); and

Retrieving from a data structure a plurality of cryptographic shares as a function of said plurality of keystroke features (see col. 2, lines 12-56; col. 3, lines 35-41).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Brown within the system of Kara to arrive at the invention as claimed because the implementation of measuring the keystroke features during entry of a password of a user would improve the ability of detecting the users who are trying to access the system, and further increase the level of security of the combined system.

33. As to claim 26, Kara does not explicitly show said cryptographic shares represent vectors. However, Brown teach wherein said cryptographic shares represent vectors (see col. 2, lines 12-51; col. 5, lines 25-29; col. 6, lines 61-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Kara in view of Brown for the same reasons set forth in claim 24 above.
rejected as above in rejecting claim 24, wherein said cryptographic shares represent vectors.

34. Claim 27 rejected as above in rejecting claim 24, wherein said cryptographic shares are compressed.

35. Claim 29 rejected as above in rejecting claim 24, further comprising the step of:

generating a plurality of indices as a function of said keystroke features (see col. 2, lines 12-56; col. 3, lines 35-41); and using said plurality of indices to identify locations within said data structure from which to retrieve said cryptographic shares (see col.2, lines 42-57).

36. Claim 30 rejected as above in rejecting claim 29, wherein said step of generating a plurality of indices as a function of said keystroke features comprises the step of:

for each of said keystroke features, generating one of two indices as a function of a threshold value (see col. 2, lines 12-56; col. 3, lines 35-41).

37. Claim 31 rejected as above in rejecting claim 29, wherein said step of generating a plurality of indices as a function of said keystroke features comprises the step of:

for each of said keystroke features, generating one of a plurality of indices as a function of a plurality of threshold values (see col. 2, lines 12-56; col. 3, lines 35-41).

38. As per claim 32, Kara does not explicitly show decrypting said cryptographic shares using said password. However, Brown teach the use of a password (see col. 2, lines 52-56; col. 3, lines 35-41). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Kara in view of Brown for the same reasons set forth in claim 24 above.

39. Claim 33 rejected as above in rejecting claim 24, further comprising the steps of:

maintaining a history file containing information relating to prior successful key generation attempts and based on said history file, storing invalid cryptographic shares in data structure locations which are not expected to be accessed during subsequent legitimate key generation attempts (see col. 2, lines 42-67 to col. 3, lines 1-25).

40. Claim 35 rejected as above in rejecting claim 34, wherein said physical measurements are measurements of DNA.

41. Claims 25 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara U.S. Patent No. 5,802,175 in view of Brown et al. U.S. Patent No. 5,557,686 ('Brown' hereinafter) in further view of Herzber et al. U.S. Patent No. 5,625,692 ('Herzber' hereinafter).

42. As to claim 25, Kara and Brown teach the limitations as above as indicated in claim 24.

Kara and Brown do not explicitly disclose wherein said cryptographic shares represent points on a polynomial.

Herzber disclose cryptographic shares represent points on a polynomial (see col. 8, lines 10-21, 46-59; col. 16, lines 39-40)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kara and Brown with the system of Herzber to arrive at the invention as claimed because points on a polynomial which have been encrypted using the expected values indicated as the encryption key would further provide an increase level of security of the encryption key from being accessed

or disclosed to unauthorized users attempting to gain access to the encryption key, further improving the security of the combined system by making it more difficult to decrypt the polynomial point with the decryption key.

43. As to claim 28, Kara and Brown teach the limitations as above as indicated in claim 27.

Kara and Brown do not explicitly disclose wherein said cryptographic shares comprise y values of points on a polynomial and the corresponding x values are derivable from a data structure location.

Herzber disclose cryptographic shares represent points on a polynomial (see col. 8, lines 10-21, 46-59; col. 16, lines 39-40)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kara and Brown with the system of Herzber to arrive at the invention as claimed because points on a polynomial which have been encrypted using the expected values indicated as the encryption key would further provide an increase level of security of the encryption key from being accessed or disclosed to unauthorized users attempting to gain access to the encryption key, further improving the security of the combined system by making it more difficult to decrypt the polynomial point with the decryption key.

44. Claims 17, 36 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara U.S. Patent No. 5,802,175 in view of Herzberg et al. (U.S. Patent No. 5,625,692).

45. Kara teach claim 17 is rejected as above in rejecting claim 11

Kara does not explicitly disclose a polynomial secret sharing scheme.

Herzberg disclose a polynomial secret sharing scheme (see col. 16, lines 39-40) wherein said cryptographic shares are cryptographic shares of a polynomial secret sharing scheme.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Herberg within the system of Kara to arrive at the invention as claimed because the implementation of a polynomial secret sharing would allow for the determination of the polynomial when the knowledge is known of a sufficient number of points on the polynomial, further improving the secret sharing schemes used to generate the cryptographic shares.

46. Kara teach claim 36 is rejected as above in rejecting claim 34.

Kara does not explicitly disclose said encrypted cryptographic share is a hash function.

Herzber disclose the use of a hash function (see col. 8, lines 26-30; col. 9,lines 35-42).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Herberg with the system of Kara to arrive at the invention as claimed because the implementation of a hash function would

enable the cryptographic share to determine the position of a given value in the set of expected index values and to calculate the hash value for the given item, further extending the capabilities and increasing the level of security of the combined system.

47. Kara teach claim 38 is rejected as above in rejecting claim 37.

Kara does not explicitly disclose said encrypted cryptographic share is a hash function.

Herzber disclose the use of a hash function (see col. 8, lines 26-30; col. 9,lines 35-42).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Herberg with the system of Kara to arrive at the invention as claimed because the implementation of a hash function would enable the cryptographic share to determine the position of a given value in the set of expected index values and to calculate the hash value for the given item, further extending the capabilities and increasing the level of security of the combined system.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gennaro et al. (U.S. Patent No. 6,317,834) disclose a biometric authentication system with encrypted models.

Mittenhal (U.S. Patent No. 6,035,042) disclose a high speed and method of providing high speed table generation for block encryption.

Follendore, III (U.S. Patent No. 5,369,707) disclose a secure network method and apparatus.

Lipner et al. (U.S. Patent No. 5,557,346) disclose a system and method for key escrow encryption).

Pearson et al. (U.S. Patent No. 5,991,408) disclose an identification and security using biometric measurements.

Tomoko et al. (U.S. Patent No. 5,712,912) disclose a method and apparatus for securely handling a personal identification number or cryptographic key using biometric techniques.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ahmedur Ali whose telephone number is 305-4667. The examiner can normally be reached on 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 305-3900.

ara

Emmanuel L. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
A/U 2136